Remarks

Entry of this amendment and allowance of all remaining claims are respectfully requested. Claims 1-4, 8-14 & 18-21 remain pending.

By this paper, independent claims 1, 11 & 21 are amended to more clearly point out and distinctly claims certain aspects of the present invention. These amendments are submitted in a *bona fide* attempt to further prosecution of the application. Support for the amended language can be found throughout the application as filed. For example, reference FIG. 11, as well as the discussion thereof at paragraphs [0081] – [0087]. Thus, no new matter is added to the application by any amendment presented.

In the Office Action, original claims 1-21 were rejected under 35 U.S.C. §102(e) as being anticipated by Cassagnol et al. (U.S. Published Application No. 2002/0129245 A1; hereinafter Cassagnol). This rejections is respectfully, but most strenuously, traversed to any extent deemed applicable to the claims presented herewith, and reconsideration thereof is requested.

By this amendment, each independent claims is revised to further characterize various aspects of Applicants' process for migrating data being encrypted using a first key set to data being encrypted using a second key set. Specifically, Applicants recite (e.g., claims 1, 11 & 21): performing multiple writes of encrypted data using a first key set; employing a usage counter to count each use of the first key set to write encrypted data; and automatically transitioning to a second key set when the count of the usage counter exceeds a defined threshold. The automatically transitioning includes: modifying an access table to indicate that encrypted data in a current data location is to be decrypted using the first key set, and is to be re-encrypted using the second key set when undergoing storage to a new data location; decrypting the encrypted data using the first key set, re-encrypting (by a data access control function within an integrated system) the data using the second key set, wherein the decrypting and the re-encrypting comprise reading the encrypted data from the current data location, decrypting the encrypted data using the first key set, then writing the data as encrypted data to the new data location employing the second key set; and modifying the access table further with the new data location being defined for encryption and decryption with the second key set. Applicants respectfully submit that numerous aspects of their above-summarized approach for migrating data from being encrypted

using a first key set to data being encrypted using a second key set are not taught or suggested by Cassagnol.

Cassagnol describes an apparatus for providing a secure processing environment. The apparatus includes a read/write memory for storing information; a first processor cooperating with a read/write memory for reading information therefrom and writing information thereto; and a cipherer in communication with a read/write memory. The cipherer is configured to selectively decrypt encrypted information into decrypted information and to deliver the decrypted information to the read/write memory for subsequent use by the first processor. The apparatus is further provided with an authenticator for authenticating the decrypted information prior to use by the first processor. (See paragraph [0011] of Cassagnol.)

Initially, Applicants note that a careful reading of Cassagnol fails to uncover any teaching or suggestion of Applicants' now-recited technique which includes performing multiple writes of encrypted data using a first key set. Cassagnol, in fact, expressly teaches otherwise. In paragraph [0057], Cassagnol states:

> Thus, one previously exported block of encrypted information is imported from the external memory 24, the whitening key used in the previous import/export cycle is used by the cipherer 20 in the decryption process. Then, when that same block of information is to be exported the cipherer 20 uses a new whitening key to perform the whitening portion of the encryption process.

In Cassagnol, the whitening key is changed with each new writing of encrypted data. For at least this reason, Applicants respectfully request reconsideration and withdrawal of the anticipation rejection to the independent claims presented herewith.

Applicants' independent claims further recite employing a usage counter to count each use of the first key set to write encrypted data. This particular aspect of Applicants' recited invention was initially presented in dependent claims 6, 7, & 16, 17, canceled herein without prejudice. In addressing this subject matter, the Office Action states at page 3:

> Cassagnol discloses a mechanism for updating the key material after a certain number of applications (see for example, [0110] – [0113]).

This conclusion is respectfully, but most strenuously traversed to any extent deemed applicable to the process recited in Applicants' independent claims. In Applicants' independent claims, a usage counter is employed to count each use of the first key to write encrypted data. No similar functionality is taught or suggested by the cited paragraphs of Cassagnol. In paragraphs [0110] – [0113], Cassagnol describes the programming of apparatus 10 loaded in test jig 122. See, for example, paragraph [0108] & Fig. 6 of Cassagnol regarding the exchange of keys between test jig and key server. Applicants respectfully submit that a careful reading of this material fails to uncover any relevancy to their recited processing. There is simply no teaching of counting each use of a first key set to write encrypted data in Cassagnol.

For this additional reason, Applicants respectfully request reconsideration and withdrawal of the rejection to the independent claims presented.

Still further, Applicants' independent claims recite automatically transitioning to a second key set when the count of the usage counter exceeds a defined threshold. Since Cassagnol fails to disclose performing multiple writes of encrypted data using a first key set, or employing a usage counter to count each use of the first key set to write encrypted data, Applicants respectfully submit that there is no suggestion to then automatically transition to a second key set when the count of the usage counter exceeds a defined threshold. To the extent relevant, Cassagnol describes at paragraphs [0056] – [0058] that the previously exported block of encrypted information is imported from the external memory 24, the whitening key used in the previous import/export cycle is used by the cipherer 20 in the decryption process, and then when the same block of information is to be exported, the cipherer 20 uses a new whitening key to perform the whitening portion of the encryption process. Thus, Cassagnol teaches using a different whitening key when re-encrypting the decrypted data. Applicants' processing advantageously provides a facility for optimizing use of the key sets by only generating and transitioning to a second key set when the usage of the first key set exceeds a defined threshold. In Cassagnol, a new whitening key is employed each time a decrypted block of data is re-encrypted.

Yet further, Applicants' process for automatically transitioning to a second key set is believed unique over the cited art. Specifically, Applicants' automatically transitioning includes modifying an access table to indicate that encrypted data in a current data location to be

decrypted using the first key set, and is to be re-encrypted using the second key set when undergoing storage to a new data location. This modification again is responsive to the count of the usage counter exceeding the defined threshold. Thereafter, the encrypted data is decrypted using the first key set, and then re-encrypted using the second key set. The decrypting and re-encrypting include reading the encrypted data from the current data location, decrypting the encrypted data using the first key set, then writing the data as encrypted data to the new data location employing the second key set. In Applicants' processing, the access table is then further modified with the new data location being defined for encryption and decryption with the second key set. No analogous processing for automatically transitioning to a second key set employing Applicants' recited updates to an access table is believed taught or suggested by the cited art.

To summarize, Applicants respectfully submit that a careful evaluation of their independent claims presented herewith leads to the conclusion that their recited invention would not have been anticipated by or obvious to one of ordinary skill in the art based on the cited art. In evaluating claimed subject matter as a whole, the Federal Circuit has expressly mandated that functional claim language be considered in evaluating a claim relative to the prior art. Applicants respectfully submit that the application of this standard to the independent claims presented leads to the conclusion that the recited subject matter would not have been anticipated by or obvious to one of ordinary skill in the art based on the applied patent. Reconsideration and withdrawal of the rejection to the claims presented is therefore respectfully requested.

The dependent claims are allowable for the same reasons as the independent claims, as well as for their own additional characterizations.

Applicants respectfully submit that all claims are in condition for allowance, and such action is respectfully requested.

If a telephone conference would be of assistance in advancing prosecution of the subject application, Applicants' undersigned attorney invites the Examiner to telephone him at the number provided.

Respectfully submitted,

Kevin P. Radigan

Kevin P. Radigan
Attorney for Applicants
Registration No.: 31,789

Dated: March 14, 2005.

HESLIN ROTHENBERG FARLEY & MESITI P.C.
5 Columbia Circle
Albany, New York 12203-5160
Telephone: (518) 452-5600
Facsimile: (518) 452-5579